PSW GROUP

Flemingstraße 20-22
36041 Fulda
Deutschland

Telefon: 0661 / 48 02 76 - 10
Fax: 0661 / 48 02 76 - 19
E-Mail: info@psw.net
Internet: www.psw.net

Ihr Ansprechpartner: Christian Heutger
Flemingstr. 20-22
D-36041 Fulda
E-Mail: support@psw.net

ONLINE-KOMMUNIKATION OFFEN WIE EIN SCHEUNENTOR:

INTERNET-DATEN VERSCHLÜSSELN!

Christian Heutger, PSW GROUP

Ihr Ansprechpartner: Christian Heutger
Flemingstr. 20-22
D-36041 Fulda
E-Mail: support@psw.net

Warum verschlüsseln?

- **Datenaustausch über das Internet …**
  - findet permanent statt
  - umfasst sensible, private Daten
  - ist meist ungeschützt
  - und daher für unbefugte Dritte einsehbar

- **Von Spionage betroffene Dienste**:

  - E-Mail, WWW, Online-Banking, etc.

Ihr Ansprechpartner: Christian Heutger
Flemingstr. 20-22
D-36041 Fulda
E-Mail: support@psw.net

Historie

- Verschlüsselung fast so alt wie die Menschheit
- Schon die alten Ägypter schützten ihre Daten
- Geheimschrift der Maria Stuart
- Enigma: Unbezwingbar aber doch geknackt
- Rasante Weiterentwicklung durch Aufkommen elektronischer Kommunikation (ab Telegrafen)
- Sprung ins Internet-Zeitalter

Ihr Ansprechpartner: Christian Heutger
Flemingstr. 20-22
D-36041 Fulda
E-Mail: support@psw.net

Verfahren: Symmetrische Verschlüsselung

- Ursprung: Ära Caesar
- Ein identischer Schlüssel für Ver- & Entschlüsselung
- Schlüssel müssen geheim gehalten werden
- Jeder Kommunikationspartner besitzt eigenen Schlüssel
- Fazit: Schnell, aber umständlich und angreifbar

Ihr Ansprechpartner: Christian Heutger
Flemingstr. 20-22
D-36041 Fulda
E-Mail: support@psw.net

Verfahren: Asymmetrische Verschlüsselung

- Ursprung: 70er-Jahre
- Zwei unterschiedliche Schlüssel
  - Öffentlicher für Verschlüsselung
  - Privater für Entschlüsselung
- Privater Schlüssel bleibt in Obhut des Empfängers (bspw. auf Server)
- Fazit: Sicherer als symmetrische Verschlüsselung, aber langsamer

Ihr Ansprechpartner: Christian Heutger
Flemingstr. 20-22
D-36041 Fulda
E-Mail: support@psw.net

Verfahren: Hybride Verschlüsselung

- Ursprung: Internet-Zeitalter
- Kombination aus symmetrischer & asymmetrischer Verschlüsselung
- Eigener Schlüssel für jede Datenübertragung
- Verschlüsselte Übermittlung des Schlüssels mit Datenpaket an Empfänger
- Fazit: Schnell und sicher
- Heutiges Einsatzgebiet: SSL

Ihr Ansprechpartner: Christian Heutger
Flemingstr. 20-22
D-36041 Fulda
E-Mail: support@psw.net

Wie verschlüsseln?

- Bei E-Mail
  - Verantwortung bei Nutzer
  - Spezielle E-Mail-Verschlüsselungslösungen
  - Verschiedene Standards: S/MIME, PGP

- Im Internet
  - Verantwortung bei Website-Betreiber
  - Mittels https:// und SSL

Ihr Ansprechpartner: Christian Heutger
Flemingstr. 20-22
D-36041 Fulda
E-Mail: support@psw.net

SSL: Die erste Generation

- Einführung: 1995
- Validierungsstärke: mittel
- Organisationsvalidierung
  - Anhand offizieller Dokumente
  - Verification Call
- Validierung auch durch RAs

Ihr Ansprechpartner: Christian Heutger
Flemingstr. 20-22
D-36041 Fulda
E-Mail: support@psw.net

SSL: Die zweite Generation

- Einführung: Um 2000
- Validierungsstärke: schwach
- Domainvalidierung
  - Abgleich mit WHOIS-Einträgen
  - Automatischer Verification Call mit PIN-Eingabe
- Vorteil: Beschleunigte Ausstellung
- Nachteil: Anfällig für Missbrauch durch Phisher
- Validierung auch durch RAs

Ihr Ansprechpartner: Christian Heutger
Flemingstr. 20-22
D-36041 Fulda
E-Mail: support@psw.net

SSL: Die dritte Generation

- Einführung: 2007
- Validierungsstärke: stark
- Erweiterte Validierung nach 4-Augen-Prinzip
  - Organisationsvalidierung
  - Domainvalidierung
  - Datenabgleich mit Telefonbucheintrag
  - Verification Call
  - Schriftliche Beantragung
  - Ggf. notarielle Beglaubigung
- Besonderheit: Einfärbung der Browser-Adressleiste
- Validierung nur durch CAs

Ihr Ansprechpartner: Christian Heutger
Flemingstr. 20-22
D-36041 Fulda
E-Mail: support@psw.net

Funktionsweise: SSL-Handshake

- Phase 1
  - Nutzer-Client fragt Server an
  - Server antwortet mit Nachricht zu u.a. SSL-Version
- Phase 2
  - Server weist sich mit SSL-Zertifikat gegenüber Nutzer-Client aus
- Phase 3
  - Nutzer-Client verifiziert SSL-Zertifikat
- Phase 4
  - Einmaliger Sitzungsschlüssel wird generiert
  - Verschlüsselte Kommunikation setzt ein

Ihr Ansprechpartner: Christian Heutger
Flemingstr. 20-22
D-36041 Fulda
E-Mail: support@psw.net

Worauf achten?

- Schlosssymbol im Browser
  - Anklickbar
  - Verschlüsselungsstärke: 256 bit
  - Schlüsselstärke: 2048 bit
- „Grüne Adressleiste“
- Regelmäßige Sicherheitsupdates des eigenen Betriebssystems
- Aktuelle Virenschutz-Software
- Einsatz einer Firewall

Ihr Ansprechpartner: Christian Heutger
Flemingstr. 20-22
D-36041 Fulda
E-Mail: support@psw.net

PSW GROUP

Flemingstraße 20-22
36041 Fulda
Deutschland

Telefon: 0661 / 48 02 76 - 10
Fax: 0661 / 48 02 76 - 19
E-Mail: info@psw.net
Internet: www.psw.net

Ihr Ansprechpartner: Christian Heutger
Flemingstr. 20-22
D-36041 Fulda
E-Mail: support@psw.net